# VANETs

Subjects: Computer Science, Cybernetics

Contributor: Muhammad Zahid Khan

A Vehicular Ad-hoc Network (VANET) comprises a group of moving or stationary vehicles connected by a wireless network. VANETs play a vital role in providing safety and comfort to drivers in vehicular environments. They provide smart traffic control and real-time information, event allocation.

Keywords: intelligent transportation system ; VANET

## 1. Introduction

In recent years, due to economic and population growth, a rapid increase has been observed in the numerous vehicles. This has automatically increased road accidents, driver exhaustion and worsening of roads and support framework. According to a healthcare report by the World Health Organization (WHO), the main cause of deaths of people between 15–29 years is road accidents, also 1.3 million people are killed in accidents annually worldwide [1]. This rapid increase in traffic accidents can be managed by practicing the latest technology to report real-time information to the driver about vehicle health parameters, circumstances of roads, traffic jams, and forewarning of weather. Progressive advancement of Intelligent Transport Systems (ITS), associated vehicles internet of vehicles known as the (IoV) [2] is the fundamental of communication required to share data about crisis and developing traffic dynamics has been expanded.

A current study by the IoT tracker service declared that the linked car market would expand by an additional 270% by 2022 including more than 125 million cars [3]. This also expands the size and complication of current working vehicle ad hoc networks, usually known as VANETs. In addition to running challenges, the rapid proliferation of vehicle connections has also created critical security and information confidentiality concerning the evolution and expansion of VANETs design. From the literature review, it can be asserted that some threats related to privacy and infringing location privacy are more dangerous as they can lead to more advanced physical attacks such as trial and robbery.

In the next three subsections, we first explain the generic VANET architecture and then its unique characteristics. We also present the motivation behind the survey and the contributions of this work.

## 2. Generic VANET Architecture

The two main communication models in VANETs are classified as Vehicle-to-Vehicle (V2V) communication and Vehicle to Infrastructure (V2I). V2V communication is the ability of exchanged transmission between different vehicles while V2I is the communication between the vehicles and the road-side framework. The main communication module consists of Road-Side Unit (RSU), on-board unit (OBU), and trusted authority (TA) as shown in Figure 1. The RSU unit is fixed and made up of a transceiver that sends and receives information from the OBU and TA.

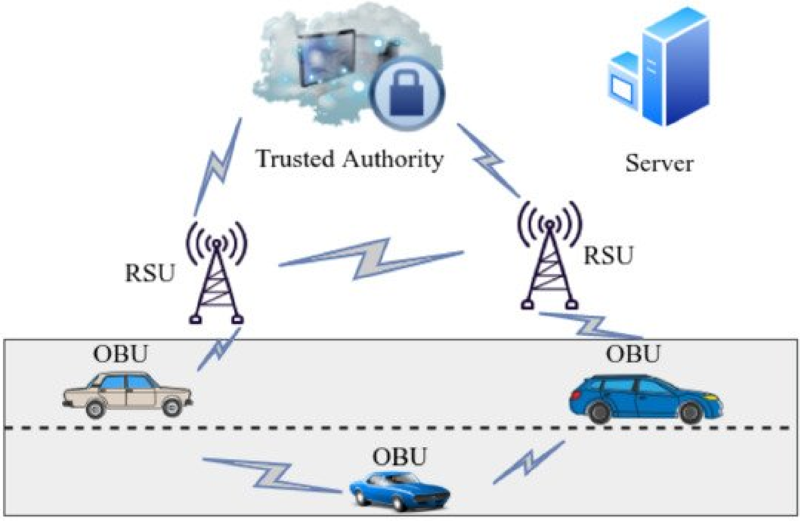

**Figure 1.** VANET Generic Architecture.

Therefore, it acts as a communication frontier between OBU and TA. RSUs can be placed at key indicators after a particular interlude to provide reliable network coverage and systematic operation. Therefore, the distance between nearby roadside units is kept within the range of each sequential RSU. OBU is fixed in the automobile and works as a central point for receiving, processing, and managing all data developed in the vehicle. It also serves as a source for exchanging data with the OBU of close-by vehicles as well as the RSU. TA is basically the foundation of the whole ITS and is usually connected to the RSU via fiber optic cable or wireless media. It manages the trust and safety of VANETs. TA verifies the entire network components via RSU and identifies the OBU that sends malicious packets and cancels the target node. TAs is in the center of the town and is managed by governments. The VANET system model is briefly described in Figure 1 below. A more detailed survey on this can be found at [4].

## 2. VANETs Characteristics

This subsection briefly explains the unique characteristics of VANET mainly mobility, storage and computing capabilities, dynamic topology, communication medium used, etc.

### 2.1. Mobility

Because VANETs nodes are highly mobile or move fast, it is often necessary to leave the localized network and participate in new configurations. These fast-moving nodes can cause intrinsic communication interruptions or retard throughout V2V and V2I communications [5].

### 2.2. Storage and Computing Capabilities

The information interchange within VANETs depends on users linked at a particular time. Therefore, network bandwidth and adequate processing power are required to store, process, and communicate important messages.

### 2.3. Real-Time Limitations

Regardless of the intrinsic delays between flexible platforms, some VANETs applications want the information to reach in real-time. For example in fault discovery and collision prevention systems where the driver has minimum reaction time (several milliseconds) available to decode and react to the received message.

### 2.4. Dynamic Network Topology

VANET’s network configuration continuously develops due to the mobility of vehicles as some nodes join and leave the network. Malicious nodes could benefit from these dynamic configurations, hiding their routes after compromising a particular network [6].

### 2.5. Frequent Network Disconnections

VANET’s most disconnections are due to other issues such as high-speed movement between vehicles and weather conditions. Many vehicles on the road can also cause frequent amputations.

### 2.6. Communication Medium

VANETs use wireless communication same as Mobile Ad-hoc Network (MANET) but the nodes involved in VANETs have more mobility as compared to MANETs. Like other wireless networks, VANETs encounter security issues because of wireless communication [7].

### 2.7. Radio Transmission Depletion

The performance of Dedicated Short-range Communication (DSRC) radio communications has limitations associated with digital transmission in these frequency bands due to dispersion, diffraction, refraction, reflection, and dispersing in city areas.

## 3. Motivation and Contribution

In VANETs, the connected vehicles and nodes of the VANETs environment contain road-side sensing and transmitting modules, traffic monitoring by the government, infotainment systems, and control systems etc. These devices share sensitive data with different protocols. VANETs are highly vulnerable to internal and external security attacks. For example, attackers can use communication to steal personal information such as passenger details, travel times, tracked routes and destinations, range, and main locations. Furthermore, this data can be used to create selected personal profiles to launch multiple attacks. These attacks can be directed towards specific users or interfere with the whole transportation system, hence blocking the flow of traffic over a vast area. For example, movements can track or disrupt through spying on the victim’s location data [8]. Therefore, location privacy in VANETs is an important design challenge to be considered.

## References

1. WHO. W. H. Organization, Global Status Report on Road Safety 2015; World Health Organization: Geneva, Switzerland, 2015.
2. Alam, M.; Ferreira, J.; Fonseca, J. Introduction to intelligent transportation systems. In Intelligent Transportation Systems; Springer: Berlin/Heidelberg, Germany, 2016; pp. 1–17.
3. Bhatia, H. 125 Million+ Connected Cars Shipments by 2022; 5G Cars by 2020. Available online: (accessed on 15 February 2020).
4. Lu, Z.; Qu, G.; Liu, Z. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans. Intell. Transp. Syst. 2018, 20, 760–776.
5. Dhamgaye, A.; Chavhan, N. Survey on security challenges in VANET 1. 2013. Available online: (accessed on 15 February 2020).
6. He, Z. Structure based or structure free? Topology management in VANETs. In Proceedings of the 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–23 September 2012; pp. 1–4.
7. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. 2014, 1, 53–66.
8. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. Veh. Commun. 2017, 7, 7–20.

Retrieved from https://encyclopedia.pub/entry/history/show/20755